

1 Pré-requis logiciel avant installation

1.1 Sur le système hébergeant « Network Shutdown Module V3 »

1.1.1 Compatibilités Windows

Network Shutdown Module V3 **Windows** est compatible avec et a été testé sur :

- Windows (x86) 2000 / XP(Home,Pro) /2003 / Vista (Professionel, Edition Integrale) / 2008 (Web Server, Standard, Entreprise, Data Center)
Windows 7,
Server 2003 Appliance Edition (Testé avec Iomega NAS Server)
- Windows (Xeon 64) Windows Server 2003 Standard x64 Edition
Windows Server 2008 Enterprise x64 Edition
Windows Vista Professionnel x64
Windows 7
- Windows (AMD Opteron) IBM blade server AMD Opteron single processor pour LS20 (type 8850)
Windows Server 2003
- Windows (Intel Xeon) IBM blade server Intel Xeon single processor pour HS20 (type 8843)
Windows Server 2003

1.1.2 Compatibilités Linux

Network Shutdown Module V3 **Linux** est compatible avec et a été testé sur :

- Linux (x86/x86_64)
Debian GNU Linux: Etch, Lenny
SUSE/Novell: SLES 11, OpenSUSE 10.3, 11.2,
Redhat Enterprise Linux: RHEL 5.4, Fedora core 12
Ubuntu: 9.04, 9.10
VMWare: ESX3, 3.5, ESXi4 (installateur NSM CLI)
Mandriva 2009, 2010

Le logiciel est basé sur les mécanismes Linux standard et peut donc être installé sur les autres distributions Linux. Les retours, tests ou rapports de bogues sont les bienvenus auprès du support logiciel EATON.

La liste suivante n'est pas exhaustive. Network Shutdown Module V3 **devrait être** compatible avec:

- Linux (x86/x86_64)
Debian GNU Linux: Testing,
SUSE/Novell: SLES 10, openSUSE 10.x, 11.x
Redhat Enterprise Linux: RHEL 4, 5 , Fedora core 10,11
Ubuntu: 7.10, 8.04, 8.04 LTS Server, 8.10
Autres: IPCop, ...

1.1.3 Compatibilités Mac

Network Shutdown Module V3 **MacOSX** est compatible avec et a été testé sur :

- Mac Intel Mac OS X 10.4, 10.5
- Mac PowerPC Mac OS X 10.4, 10.5

1.1.4 Configuration de la mise en veille (Windows):

Dans Démarrer-> Paramètres -> Panneau de configuration -> Options d'alimentation:

- Vous devez désélectionner la configuration de la mise en veille pour votre système d'exploitation. Lors de la mise en veille, votre système n'est plus protégé.
- Si vous souhaitez économiser de l'énergie, choisissez alors la fonction Mise en veille Prolongée (hibernate).

1.1.5 Broadcast Message configuration (Windows)

Si la fonction "[Broadcast administrator messages / Broadcast user messages](#)" est activée sur le Network Shutdown Module, vous devez vérifier que le service "Affichage des messages" est démarré. Ce service doit être démarré pour utiliser la fonction envoi de message sous Windows.

1.1.6 Paramétrage Firewall (Windows & Linux) et Passerelle

(Optionnel) Pour permettre un accès distant pour configuration et supervision, le Network Shutdown Module nécessite d'ouvrir les ports UDP et TCP au niveau du Pare-feu :

- **4679** EATON Supervision
- **4680** EATON Management (SSL)

Ces ports sont réservés pour EATON auprès de IANA (Internet Assigned Numbers Authority <http://www.iana.org/>).

Si vous utilisez Windows, les ports sont automatiquement ouverts dans le Pare-Feu de Windows.

Si vous utilisez un Firewall dont tous les ports sont bloqués par défaut:

Pour la communication entre Network Shutdown Module et Network Management Card:

- Le port 80 doit être ouvert en tant que port "destination" (en sortie) sur la machine hébergeant Network Shutdown Module.

Si vous utilisez une passerelle dont les ports ne sont pas routés par défaut:

- Assurez-vous de router les ports 4679 et 4680 avec le protocole «TCP» & «UDP»

1.2 Sur le système affichant l'interface utilisateur Web

Important :

L'interface graphique peut être visualisée à distance en utilisant un simple navigateur Web. L'accès à cette interface est sécurisé par une connexion SSL (par défaut) et **doit** également être protégée par [compte utilisateur et mot de passe](#).

L'interface graphique de Network Shutdown Module a été testée avec:

- Mozilla Firefox 1.5, 2.0, 3.0 recommandé pour de meilleures performances. (**Firefox obligatoire avec Linux**)
- Microsoft Internet Explorer V 6, 7 & 8
- Safari

Note : Pour le navigateur Web, l'utilisation du niveau de sécurité le plus élevé est déconseillée. Certains écrans de configuration sont alors inutilisables.

Javascript et les Cookies doivent être autorisés pour le niveau de sécurité sélectionné